

ABSTRACT OF THE DISCLOSURE

A security switch detects whether requested content is either trusted content or non-trusted content. In case of network content being trusted content, network traffic bypasses the inspection gateway and goes directly to the user. If network content is non-trusted content,
5 network traffic passes through to the inspection gateways for inspection. Additionally, when the security switch receives a reply for “trusted” content requests, it parses the reply information to verify that the content-type of the file is indeed “trusted”. If the file doesn’t prove to be “trusted”, the security switch drops the connection and stops the suspected content from reaching
10 the client.